REMARKS/ARGUMENTS

Reconsideration of the application is respectfully requested. Claims 1-2, 4-27 were rejected under Section 102 as being anticipated by Kunzinger. This rejection is respectfully traversed. Claims 28-29 have been added to the application. No new matter has been added to the application.

Applicants submit that Kunzinger merely teaches end-to-end protection between the client and the server when the flag cannot be set and the use of cascaded tunnels (see abstract) when the flag can be set in which, as shown in Fig. 4, a first tunnel extends between the first computer (client) and the intermediate computer (boundary device or gateway) and a second tunnel extends between the intermediate computer and a second computer (server). The first tunnel provides security through the Internet and the second tunnel provides security through an intranet (see paragraph [0051] of Kunzinger). Kunzinger explains in paragraph [0047] that the "use of cascaded tunnels (as opposed to one tunnel or SA extending from the client to the server) allows security protection to be tailored to the requirements of a particular network segment." He also explains that the security gateway serves as a point of entry into the intranet (paragraph 0050) and that the security gateway 420 retains the ability to provide of the type of services available in the environment

of Fig. 3. These services include access control and network address translation that require content inspection. In other words, the gateway protects the intranet from undesirable communication from the open Internet by inspecting the content of incoming packets before the packets enter into the intranet. This requires the gateway (intermediate computer) to decrypt the incoming packet in order to be able to inspect the content of the incoming packet. In the current invention, the intermediate computer does not need to know the cryptographic keys or read the content but is able to use the outer IP addresses and the incoming SPI value (= unique identity) to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination.

In paragraph [0013], Kunzinger explains that the security associations are negotiated between the tunnel endpoints i.e. a first negotiation is between the endpoints of tunnel 1 and a second negotiation is between the endpoints of tunnel 2. This means the client 405 negotiates with the gateway 420 to establish tunnel 1 (but not with the server 440). Similarly, the gateway 420 negotiates with the server 440 to establish tunnel 2.

As indicated above, Kunzinger clearly teaches the advantage of using cascade tunnels which provide the tailoring features (see paragraph [0047]) "as opposed to a tunnel or SA extending from the client to the server." Also, in paragraphs

[0012-0014] Kunzinger explains that each tunnel is a separate connection. Also, in paragraphs 0067-0068 Kunzinger explains if there is no existing cascaded tunnel available between the gateway 420 and the server 440 then a pair of IKE and IPSsec security associations are established to provide the next tunnel (which again indicates that there are two separate tunnels and not one tunnel).

On page 4 of the Office action, the Examiner states that Kunzinger's key is equivalent to the "first unique identity" required in the claim 1. Applicants are still puzzled over this statement. A key is something used for encryption and decryption (lock and unlock). It is submitted it would not make sense to send a secure message that includes the key in the same message. If the key is sent together with the encrypted message then the encryption would be meaningless since anyone would have access to the key and would be able to decrypt and read the encrypted secure message. A key therefore does not need to be sent in the same encrypted message. It could be like leaving the key in a locked door when leaving your house. Also, if the key were sent as data in the encrypted message, then the recipient could not gain access to the key included in the encrypted message because the recipient could not gain access to the key either to be able to decrypt/open the encrypted message. It is therefore submitted that the key in Kunzinger does not correspond to the unique identity of the present invention and that the key in

Kunzinger would not be contained in the secured message since the amended claim 1 now requires that the secure message contains the first unique identity and the first destination address. Support may, for example, be found in paragraph [0043] and the original claim 7 of the published US 2006/0173968.

Claim 1 has also been amended to specify that there is a secure connection between the first computer and the second computer via the intermediate computer. Support may be found in paragraph [0075] which states that an IPSec connection is formed between the first computer and the second computer. As clearly shown in Fig. 4 of Kunzinger, his system has two connections when the flag can be set, one tunnel between the client 405 and the gateway 420 and a second tunnel between the device 420 and the gateway 440. More particularly, the amended claim 1 requires the step of "the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer." This means that there is a secure connection in the present invention that extends between the first computer and the second computer. Thanks to the unique features of the present invention, the secured information flow can work all the way from the first computer to the second computer even if there is an intermediate computer therebetween.

In contrast, Kunzinger teaches two (or more) successive secure connections (IPSEc tunnels one after another). As indicated above, this is clearly shown in Fig. 4 of Kunzinger wherein the first secure connection (Tunnel 1) extends between the client (the first computer) and the gateway (the intermediate computer) and the second secure connection (Tunnel 2) extends between the gateway and the endpoint (the second computer). In other words, each tunnel is a separate secure connection, as explained very well in paragraphs [0012] and [0014]. This means there is no direct secure connection extending between the client 405 and the server 440 in Kunzinger when the flag is set. This interpretation is verified in Kunzinger's claim 1 and abstract. Of course, as indicated earlier, Kunzinger expressly teaches away from using such a secure connection when the flag is set since the intermediate gateway 420 would be prevented from access, as explained in paragraph [0017].

In Kunzinger there is thus not any key negotiation between the client 405 and the server 440 when the flag is set. In contrast, the client 405 first changes keys with the gateway 420, and thereafter, the gateway 420 exchanges keys with the server 440. Please also see Fig. 11 and paragraphs [0071 - 0074] of Kunzinger.

On page 2 of the Office action, the Examiner states that Kunzinger teaches a direct key exchange between a first computer (client in Kunzinger) and a second computer (server

in Kunzinger). However, paragraph [0072] referred to by the Examiner teaches that if cascading-enabled flag is not set, the packet will be forwarded as in prior art. The prior art method is described in paragraphs [0050-0051] and in Fig. 3 of Kunzinger. Fig. 3 clearly shows that the secure tunnel (Tunnel 1) is between the client and the gateway (equivalent to the intermediate computer of the present invention). So the key exchange to establish the secure connection takes place between the client and the gateway in Kunzinger (when cascading-enabled flag is not set) and not between the client and the server via the gateway, as required by the amended claim 1. It should be noted that the prior art technology Kunzinger is referring to when the flag cannot be set is described in Figs. 1-3, 5 and 7 and not the prior art technology described in paragraph [0017], lines 1-3. Paragraph [0017] merely mentions the possibility of extending the security association between the client and the server but Kunzinger never teaches that this end-to-end protection is to be used when the flag cannot be set. Even if Kunzinger did teach this, Kunzinger still fails to teach or suggest sending a message that contains the unique identity and using this unique identity to identify the address to the second computer.

It is submitted that the secure tunnel (Tunnel 1) in Fig. 3 could extend between the client and the server because in Kunzinger, the gateways has clear text access to datagrams

as explained in paragraph [0027], lines 13-15. If the tunnel would be between the client and the server, then the gateway would not have clear text access to the datagrams. In paragraph [0017], Kunzinger explains that there are several disadvantages in providing an end-to-end security association between the two end-points (i.e. between the client and server, see paragraph 0017) because any "intermediate system in the network path are prevented from accessing the clear-text data content of the transmitted packets, because only the two endpoints are able to encrypt and decrypt the packets on this SA." In other words, Kunzinger expressly teaches away from a security association that extends between the client (first computer) and the server (the second computer) when the flag is set which is the only time the gateway would be using the id to identify the second computer. A secure connection that extends between the first computer and the second computer is exactly what is required by the amended claim 1 and that the intermediate computer uses the unique identity contained in the secure message to find the address to the second computer.

Applicants fail to see why a person of ordinary skill in the art would look to Kunzinger to learn about establishing a secure connection between the first computer and the second computer in which the first computer is the first end-point and the second computer the second end-point and the intermediate computer using the unique identity

contained in the secure message to find the address to the second computer when Kunzinger expressly teaches away from this feature when the flag is set since the intermediate computer would be prevented from accessing the clear-text data content described in paragraph [0017]. When the flag is not set the gateway would not use any unique identity contained in the secure message to find an address for the second computer.

It is noted that the Examiner has split up the step of "the first computer and the second computer negotiating and exchanging keys with one another according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer." First, the Examiner states that the direct communication is taught in Kunzinger when the cascade-enabled flag is not set [see paragraph 0072] and then the use of intermediate computer is taught when cascade-enabled flag is set (see paragraph [0068]). The use of cascade-enabled flag is clearly mutually exclusive since it cannot be on and off at the same time so the teaching of paragraphs [0072] and [0068] cannot be combined in the manner suggested.

It is also noted that the Examiner has not commented on all the arguments presented in the previous response. The Examiner is respectfully requested to review and consider all the arguments presented.

On pages 3-8 of the Office action, the Examiner refers to paragraphs [0067] and [0068] of Kunzinger. However

the cited paragraphs, among other things, explain that the gateway decrypts that incoming data packet by using the decryption key that corresponds to the particular secure association i.e. Tunnel 1 extending between the client and the gateway. Kunzinger then explains that whether the message is intended to be forwarded further in the secured form (to the endpoint) then a Tunnel 2 has to be used and if there is no Tunnel 2 then it has to be established by means of a key exchange (IKE) procedure. Kunzinger explains that the policy "will direct the gateway to either use an existing cascaded tunnel, or if one is not available, to establish a pair of IKE and IPsec security associations that will provide this next cascaded tunnel. Kunzinger is here referring to Tunnel 2. This again confirms that Kunzinger teaches two separate tunnels (secure connections) and it is submitted that it would not have been possible for Kunzinger's gateway to have decrypted the packet had the tunnel extended all the way between Kunzinger's client and server.

In several places of the Office action, the Examiner refers to paragraph [0013] of Kunzinger. This paragraph explains what an IPsec packet generally consists of. More importantly, the paragraph explains that the negotiation takes place between the tunnel endpoints. This means there is no secure connection negotiation between the client and the server since the first tunnel (Tunnel 1) ends at the gateway and the second tunnel (Tunnel 2) only extends between the

gateway and the server. In other words, the negotiations take place between the client and the gateway regarding Tunnel 1 and between the gateway and the server regarding Tunnel 2 since those represent the endpoints of the two tunnels when the flag is set and the gateway is actively involved. The amended claim 1 requires negotiation between the first computer (Kunzinger's client) and the second computer (Kunzinger's server) since the current invention needs only one secure connection even if there is an intermediate computer between the endpoints of the secure connection. It is submitted that Kunzinger fails to teach or suggest all these steps.

It is submitted that Kunzinger would require extensive modifications that are not taught or suggested to arrive at the features of the present invention. Applicants fail to see why a person of ordinary skill in the art would look to Kunzinger to learn about the secure connection and the key exchange between the first and second computer when Kunzinger completely fails to teach or suggest these and other steps of the amended claim 1.

In view thereof, claim 1 is submitted to be allowable.

Claims 2, 4-21 are submitted to be allowable because they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited references.

Independent claim 22 is submitted to be allowable for reasons similar to the reasons put forth above. Claim 22 has been amended to now require that the secure message contains the unique identity and that the intermediate computer has a module performing the IPsec and IKE translation etc. without decrypting the secure message. Support for this limitation may be found in paragraph [0085].

In contrast, the intermediate computer in Kunzinger decrypts the incoming secured message, as explained above. An important function of Kunzinger's gateways is to function as a port of entry into an intranet and to inspect the content of incoming secure packets which requires decryption of the packets before forwarding them to the server (the second computer) in the intranet. In other words, the decryption is an important function of Kunzinger's invention because the security gateway (intermediate computer) must be able to decrypt the packet so that it can provide the important services of access control, network address translation etc. that require content inspection, as explained in for example, paragraph [0050] of Kunzinger. Throughout the Kunzinger patent, the feature of content inspection is emphasized and it is submitted it would be contrary to the spirit of Kunzinger to modify his system to prevent the security gateway from being able to inspect the content of the incoming packets. It is submitted that Kunzinger would require extensive modifications that are not taught or suggested in the cited

references in order to meet the requirements of the amended claim 22.

Claims 23-26 are submitted to be allowable because they depend upon the allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

Independent claim 27 is submitted to be allowable for the same reasons as those put forth for the patentability of claim 22. In addition, the amended claim 27 requires a module for performing the IPsec and IKE translation etc. without undoing the IPsec processing and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new IPsec connection and that the secure message contains the unique identity. Support for these amendments may, for example, be found in paragraphs [0045, 0047, and 0073].

Claim 3 was rejected under Section 103 as being obvious over Kunzinger in view of Patel. This rejection is respectfully traversed.

Claim 3 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the cited references.

New claims 28-29 are submitted to be allowable because they depend upon the allowable base claim 1 and because the claims include limitations that are not taught or

suggested in the cited references. Support may, for example, be found in paragraphs [0047 and 0053] of the current application.

Paragraph [0074] of Kunzinger explains that a second successive secure connection is established (to create Tunnel 2), since there is a new key exchange performed between the gateway and the server and the copied values (IDci and IDcr) from the SAD database from Tunnel 1 are used to create Tunnel 2. To be able to fully understand paragraph [0074], the Examiner is requested to also review paragraphs [0068] and [0069] first. Paragraph [0068] explains that "when a data packet arrives from the client at the gateway, the gateway can decrypt that packet using the decryption key corresponding to the IPSec SA established with the client on the Tunnel 1 side. At this point in the process, the gateway is in possession of a clear text copy" of the message with the start address 9.1.2.3. (=the client's address, i.e. the first computer) and the destination address 8.1.2.3 (the server''s address, i.e. the second computer). Paragraph [0068] further states that the gateway is directed to use an existing tunnel or to establish a pair of IKE and IPSec security associations that provide the next tunnel. Paragraph [0069] explains if the message has to be sent further as an IPsec, then the gateway plays the role of an IKE initiator for the purposes of establishing an IPsec SA with server (which is the endpoint). Kunzinger thus teaches the gateway establishing a new tunnel

(secure connection) and the gateway involves the server (the second computer) which is opposite to what is required by the new claim 28.

In view thereof, claims 28-29 are submitted to be allowable.

The application is submitted to be in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1078USN

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

Telephone: (910) 687-0001
Facsimile: (910) 295-2152

It is submitted that Kunzinger and the other cited references fail to teach or suggest the step of the first and second computers exchanging keys with one another to establish the secure connection that has a source address of the first computer and a destination address of the second computer.

On page 4 of the Office action, the Examiner has interpreted paragraph [0013] of Kunzinger so that the IPsec inner header specifies the end points of the secure connection. However in paragraph [0013], it stated that the outer IP header specifies the end points of the tunnel (which is the secure connection in that context) and the inner header specifies the original source and the destination of the packet (so outside of the tunnel of those packets can be clear text).

Again, the examiner says that the key is the id, but in IPsec none of the messages contains any keys. Maybe we should ask the examiner to show where it is taught to put keys in packets? Or we could clarify the feature so that the unique identity must be in message?

REPETITION OUR FORECOING INSTRUCTIONS
Please make use pf them again and try to convince the examiner. He has not commented the most of our response:

When we, in our invention as claimed, "give the secure message an unique identity and a first destination address to the intermediate computer", we mean information that is outer information outside the enerypted message.
The Examiner says that "the key is the id". This is, however, of no sense. A key is a tool that is used to decrypt (remove encryption) from an encrypted message.

As a summary we show in an illustrative way the differences between the invention and Kunzinger. Differences in our invention underlined.

	Our invention	Kunzinger
Message data	IPSec encrypted= IPSec message	IPSec encrypted= IPSec message
Outer IP header in IPSec message (outside encrypted	the source address= first computer	the source address= first computer

message data(	the destination address= intermediate computer	the destination address= intermediate computer
Inner IP header in IPSec message (inside encrypted message data)	the source address= first computer the destination address= second computer	the source address= first computer the destination address= second computer
Inside outer IP header but outside inner IP header = in unencrypted part being outside information	Unique identity	No unique identity
Intermediate computer action	- No decryption of IPsec message -Finding address of second computer to be the new destination address by means of unique identity - Changing destination address in outer IP header to address of second computer	- Decryption of IPsec message - Finding address of second computer to be the new destination address by reading from Inner IPSec header - if found address not in use -> translating address by means of a table - creating new IPSec SA from intermediate to second computer by performing key exchange and IKE and -creating new outer and inner IP headers Or using an already established IPSec SA from intermediate to second computer
New outer IP header	the source	the source

	address= the intermediate computer the destination address= the second computer	address= the intermediate computer the destination address= the second computer, which might be a translated address, see above.
New inner IP header	the source address= first computer the destination address= second computer (Not changed!!!)	the source address= the intermediate computer the destination address= the second computer

Final comments
As is explained in the table, in Kunzinger, the message is decrypted by the intermediate computer
And the intermediate computer uses another tunnel 2, which has to be separately established to sent the message further with IPSec.

Claim 1 has been amended to clarify that the first computer and second computer negotiate and exchanges key with one another to establish the secure connection. Support may be found in, for example, paragraphs 0075-0093 of the corresponding published US 2006/0173968. The secure connection extending between the first computer and the second computer is shown in Fig. 1.

In view thereof, Applicants even submit that Kunzinger teaches away from the first computer and the second computer negotiating and exchanging keys with one another to establish a secure connection between the first computer and

~~the second computer. More particularly, Kunzinger fails to teach or suggest the direct exchange of keys between the client 405 and the server 440. The key exchanges described in Kunzinger are only between the client (first computer) and the gateway (intermediate computer) to establish tunnel 1 and then between the gateway (intermediate computer) and the server (second computer) to establish tunnel 2. In other words, in Kunzinger the client 405 first exchanges keys with the gateway 420 (intermediate computer) and thereafter the gateway 420, in turn, exchanges keys with the server 440 (the second computer). There is thus no direct exchange between the client 405 and the server 440 to establish a tunnel between the client 405 to the server 440. There is therefore no key exchange between the client and the server either.~~

~~Independent claims 22 and 27 are submitted to be allowable for reasons similar to the reasons put forth for the allowability of the amended claim 1. More particularly, it is submitted that none of the cited references teaches means for directly exchanging and negotiating keys between the first and second computer. As explained above, an important function of Kunzinger's gateways is to function as a port of entry into an intranet and to inspect the content of incoming secure packets which requires decryption of the packets before forwarding them to the server (the second computer) in the intranet. There should therefore be no direct communication between the client and the server since the role of the gateway is to~~

~~inspect the incoming packets before they enter the intranet.~~

~~In view thereof, claims 22 and 27 are submitted to be allowable.~~

~~Summary~~

~~As is stated in [0013] of Kunzinger, A message that is sent with IPSec contains~~

~~- Message data~~
~~- An outer IP header with~~
~~- the source address~~
~~- the destination address~~
~~- An inner IP header with~~
~~- the source address~~
~~- the destination address~~

~~Both our invention and Kunzinger have a first computer (Kunzinger's client), an intermediate computer (Kunzinger's gateway) and a second computer (Kunzinger's server)~~

~~Also, please look at the table above, then it is understood what is meant by network translating in Kunzinger. Sometimes an endpoint address is just not right since e.g. a LAN uses the same endpoint address for each computer in the Local Area Network, officially and if a certain computer in the LAN is wanted to reach, a network translation has to be done. But this network translation has nothing with the IPSec message's IP headers to do.~~

~~The advantages are that, no new IPSec (no new tunnel has to be established or used) and that the intermediate computer can forward the message in IPSec form without reading the message (which is a security question, too and improves the security).~~